CYBER SPACE: RESHAPING THE CONTOURS OF INTERNATIONAL POLITICS

ASHISH GUPTA

The inherent uncertainty and complexity of international politics underpins the importance of focussing on contemporary and emerging issues which have a bearing upon international global collaboration and harmonisation of interests. International Relations (IR) are shaped by states' differing perceptions of each other[1] and are tied to states' overriding concerns to secure their vital interests. Although strategic narratives in IR and foreign policy do not accord a central role to science and technology, there is enough undeniable evidence to highlight the causative influence of technological innovations on responses and approaches between nations. The techno-political mismatch among nations, in terms of both level and structure of this mismatch, is manifesting in rearticulation of traditional IR narratives. The developments in technology, both centrally and peripherally, impact contemporary global affairs and the collective efficacy of the commitments of states for amicable and consensual resolution of disputes and differences. Various issues within the gamut of IR are embedded in technological infrastructures developed by nations to enhance their security and standing in the global world order, reminiscent of the Cold War era as well as reflective

Group Captain **Ashish Gupta** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

1. Alexander E. Wendt, "Anarchy is what States Make of It: The Social Construction of Power Politics", *International Organization*, vol. 46, no. 2, Spring 1992, pp. 391–425.

For a nation, attainment of a respectable and dominant position in global political networks is largely linked to its technological prowess. It was technological superiority that expedited the colonialism of regions tied up with antiquated or obsolete technology.

of current geopolitical arrangements. In order to elicit an insightful appreciation and a clearer understanding of the inherent implications, there is a need to impute new meaning to old concepts and use new concepts to convey old meanings; exegetically and contextually modified to suit an increasingly techno-centric global environment.

The sequential technological revolutions facilitated the human evolutionary journey of becoming the most dominant species on planet earth.[2] At the onset of the so-called 'modernity', the rise of nations is largely attributable to wealth and power accrued through scientific and technological innovations and exploitation. For a nation, attainment of a respectable and dominant position in global political networks is largely linked to its technological prowess. It was technological superiority that expedited the colonialism of regions tied up with antiquated or obsolete technology. The exploratory sea voyages of the 15th and 16th centuries—initially by the Portuguese, and later by the Spanish, English, French, Dutch and others—turned out to be the precursors of a long and oppressive regime of colonialism and imperialism. This became possible due to assimilation and exploitation of superior technology for design and construction of naval ships and weapons. During these periods, technologies and scientific innovations served as tools of imperialism and foreign domination, and in both direct and subtle ways, changed the global demographic structure, geopolitical equity and the socio-economic divide.

The famous historian Edward Gibbon argued that in 18th century Europe, the development of the technical arts and their adaptation by rival European states, made military success a matter more of superior

2. Kevin Robins and Frank Webster, *Times of the Technoculture: From the Information Society to the Virtual Life* (London: Routledge, 1999), p. 9.

technology than military virtue.[3] This also helped to rid Europe of the scourge of nomad incursions that threatened the very existence of the European civilisation, since the superior 'rude valour' of the barbarians could not match the technological developments and military balance tipped in favour of static civilisation.[4] Lynn White has argued that as a means of understanding medieval history, the focus should remain on the dynamics of the technological changes shaping transnational and local interactions/engagements rather than on texts of that period.[5]

The technological developments in the beginning of the 20th century, played a decisive role in the unfolding of political events across the globe that culminated in two World Wars and eventually led to the downfall of Western Europe as the centre of world power.

The technological developments, in the beginning of the 20th century, played a decisive role in the unfolding of political events across the globe that culminated in two World Wars and eventually led to the downfall of Western Europe as the centre of world power. In the run-up to the wars and during the wars themselves, both sides tried innovations in technologies. During World War I, to break the standoff, both sides used artillery barrages, chemical weapons, strategic bombing and even primitive tanks. World War II proved even more technologically transformative: a watershed in technology and human history. The list of technology innovations includes: microwave radar, jet propulsion, proximity fuses, guided missiles, acoustic torpedoes, and, of course, the atomic bomb.[6]

At the turn of the 20th century, a new and pervasive information revolution emerged worldwide, redefining the global political order and representing a profound political and societal 'paradigm shift'. Alvin Toffler, eloquently and compellingly wrote about the transformation of the

3. Oliver Stuenkel, *Post-Western World: How Emerging Powers Are Remaking Global Order* (Cambridge: John Wiley & Sons, 2016), p. 56.
4. Lucian M. Ashworth, *A History of International Thought* (New York: Routledge, 2014), p. 55.
5. Lynn White Jr, *Medieval Technology and Social Change* (Oxford: Oxford University Press, 1962), p. 67.
6. Alex Roland, *War and Technology* (New York: Oxford University Press, 2016), pp. 78-83.

The increasing sophistication and strategic penetration of ICT and the internet is reshaping the contours of the global political order and restructuring the global cultural ambience. This disruptive technology has brought about a paradigm shift in global commerce, unprecedented in magnitude, spatial extent and temporal scale.

"infosphere" with the addition of a whole new strata of communication to the social system.[7] This transformed and evolving infosphere, combined with the phenomenon of an all pervasive digitisation, is redrawing the fundamental parameters of society, economy, and politics.[8] The new Information and Communication Technology (ICT) has shrunk geographical distances, increased the speed of communication and transformed the world into a global village. However, the rapid globalisation and integration, expedited through ICT, is paradoxically widening the economic and social gaps, placing the digitally endowed societies with unbridled access to ICT networks in an advantaged socio-economic and political position. Besides, a number of private entities in the ICT sectors have amassed frightening amounts of power and influence and have leveraged this to subvert efforts to distribute ICT resources in just and equitable ways.

The positions occupied by the nations in the global power hierarchy are inherently based on relational determinants. In global politics, equations of power yield perceptible solutions when subdivided into separate thematic areas of comparable parameters.[9] This may entail who is empowered versus who is disempowered (instrumental power); who is constrained in a given situation versus who gets to write the rules (structural power); and, finally, how basic identities, interests, and issues themselves are reconstituted or transformed in particular historical contexts, in turn, redefining other relations of power (called meta-power).[10]

7. Alvin Toffler , *The Third Wave* (New York: Bantam Books, 1981), p. 172.
8. J N Rosenau, and J P Singh, eds., *Information Technologies* and *Global Politics*: *The Changing Scope of Power and Governance* (Albany: State University of New York Press, 2002), p. 143.
9. Ibid., p. 6.
10. Ibid.

The ever-spreading tentacles of the internet have become so entwined in virtually every facet of social, economic and political activities that for a majority of the population, loss of cyber space tantamounts to a crisis of existential proportion. The increasing sophistication and strategic penetration of ICT and the internet is reshaping the contours of the global political order and restructuring the global cultural ambience. This disruptive technology has brought about a paradigm shift in global commerce, unprecedented in magnitude, spatial extent and temporal scale. As with any new paradigm shift, there are the naysayers as well as the enthusiasts. It turns out that the aphorism is true in the context of cyber space also, as some are hopeful of a brighter future shaped by the technological developments; others are worried due to the possible loss of jobs and concern about a "digital divide," a chasm between those who are digitally affluent and those who are not, within and between countries.

The sustained technological developments contribute to the empowerment of a state, fuel its territorial aspirations and provide an impetus to broaden its global footprint. These can also exacerbate the imbalance between technologically advanced and less technologically advanced nations. At a deeper and less perceptible level, technology can alter the identity and influence of a nation, either through greater empowerment within the existing global political structure or buttressed by technology redefining the very nature of power. The role of nuclear weapons – implicitly of technology—in ending World War II, launching the Cold War as well as establishing a world order dominated by the two superpowers highlighted the importance of technological prowess for strategic gains. The national pride of the superpowers was riding on the success and achievement of milestones in the field of technology. During the period of the Cold War, there was an ongoing contest among the superpowers without any overt military confrontation. During the 1950s, the nuclear arms race became the pivot around which most of the acts of the superpowers (and their allies) against each other were undertaken. The nuclear race was further exacerbated when the US tested the first hydrogen bomb in 1952. Similarly, there was fierce and vicious competition during the early space race. The American psyche was

severely scarred in the aftermath of the successful launch of the Sputnik—the first artificial satellite—by the USSR. In order to restore American pride, President John F. Kennedy called for the US to commit itself to achieving the goal of landing a man on the moon and returning him to earth before the end of the decade. The landing of Apollo 11 on the moon on July 20, 1969, assuaged the American pride.

During the latter part of the 20th century, the world witnessed an information revolution, facilitated by the internet and supported by the ubiquity and affordability of electronic devices. Although this revolution is the product of a long evolutionary process of innovations and modifications, some of its characteristics suggest a sharp break from the past.[11] The information revolution is a pervasive feature today and has changed the contextual setting in which international relations are conducted.[12]

INFORMATION REVOLUTION: CHALLENGING THE WESTPHALIAN NOTION OF SOVEREIGN NATION-STATES

The 'Peace of Westphalia' is a watershed in modern history, resulting in provincial readjustments, geographical arrangements and establishing territorial sovereignty demarcated by borders. Under the 'Peace of Westphalia', a series of peace treaties were signed in the year 1648 in Osnabrück and Münster in Germany, ending the Eighty Years' War between Spain and the Dutch Republic and Thirty Years' War in the Holy Roman Empire. In the later centuries, the concept of sovereignty, as enshrined in the treaty, became the basis of guiding principles for nation states. However, the fluidity of the geopolitical landscape, exacerbated by the political, strategic and economic compulsions, resulted in redrawing of national boundaries among many neighbouring nations. Nonetheless, the current world order ensures sovereign control of a nation over its territory.

But the internet shook the very foundation of sovereignty as propagated by the dominant Westphalian conceptions. The unhindered and unencumbered

11. Elizabeth C. Hanson, *The Information Revolution and World Politics* (Maryland: Rowman & Littlefield Publishers, 2008), p. 1.
12. Ibid.

character of the internet transcended physical boundaries with impunity and hubris. The virtual space used by the internet and its operatives became so well entrenched in consciousness and life that it was even christened with an appropriate name: cyber space. There is a growing clamour to identify it as one of the 'Global Commons' at par with the High Seas; the Atmosphere; Antarctica and, Outer Space, outside of the political reach of any one nation state. Independence was the structural yarn used for weaving the fabric of the internet as we know it today. The agnostic nature of the used standards and protocols does not differentiate among creed, culture or countries. An attempt to block the internet traffic is treated as a technology hitch and the traffic is rerouted through seemingly infinite networks. "The Net interprets censorship as damage and routes around it."[13] There is a widely held view that it "is not a physical place—it defies measurement in any physical dimension or time-space continuum. It is a short-hand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[14]

In the real world, the notion of a 'frontierless' world is a utopian construct and it is simply matter of time for realisation to dawn that only good fences make good neighbours. Cyber space is no exception and border delineation efforts have already begun, albeit with ambiguity regarding the final outcome.

In the real world, the notion of a 'frontierless' world is a utopian construct and it is simply matter of time for realisation to dawn that only good fences make good neighbours. Cyber space is no exception and border delineation efforts have already begun, albeit with ambiguity regarding the final outcome. The US is unwilling to give up its dominant role, acquired partly

13. "John Gilmore's Maxim," http://techpresident.com/networked-public-sphere. Accessed on January 20, 2017.
14. Thomas C. Wingfield, "The Law of Information Conflict: National Security Law in Cyberspace," Aegis Research Corporation, 2000.

Paradoxically, the Communist Party of China, while being wary of the implications of unrestricted online access to information to its legitimacy, has enthusiastically promoted the use of the internet as an inalienable part of its quest for global hegemony, economic growth and orchestration of its technical prowess.

through the accrued advantages from the efforts during the development phase of the internet and partly from the location of critical infrastructure such as root name servers in the US and in countries closely allied with the US. Many nations have clamoured for years to get rid of US dominance and have sought a more assertive role for themselves on issues related to internet governance. However, the US has been thwarting any move it sees as an organised effort by other nations to wrest control of one centralised resource of the internet that was both "unilateral and centred in the US".[15] China has its own home-grown Internet walled from the rest of the world. In less democratic states, the content control over the internet and censorship has become the norm. Traditionally, institutionalised centres of power have resorted to censorship of information and after sieving the information through the mesh of their perceived values and interests, made it accessible to the masses. A similar kind of censorship is now being practised over the internet to block, filter or censor access to information, to disseminate misinformation or to create a system of mass surveillance.

In the case of China, it has an ambivalent attitude towards the internet. China views the internet as a fertile ecosystem that germinates, fosters, nurtures and engenders political dissent, detrimental social activities and societal unrest. During the Arab Spring in early 2011, China bolstered its censorship bureaucracy, reportedly creating a new office under the State Council Information Office to "regulate every corner of the nation's vast Internet Community."[16] China's new internet czar is Lu Wei who took

15. M. L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge: MIT Press, 2010), p. 75.
16. Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (New York: Cambridge University Press, 2014).

over the State Internet Information Office in 2013 and became the director of a powerful internet committee headed by President Xi Jinping in 2014.[17] While unrepentantly defending China's need for stronger internet content control, he issued new regulations restricting sharing on social media sites and increasing censorship of popular online video sites. In response to criticism of such controls, Lu Wei said, "The internet is like a car. If it has no brakes, it doesn't matter how fast the car is capable of traveling, once it gets on the highway, you can imagine what the end result will be."[18] Paradoxically, the Communist Party of China, while being wary of the implications of unrestricted online access to information to its legitimacy, has enthusiastically promoted the use of the internet as an inalienable part of its quest for global hegemony, economic growth and orchestration of its technical prowess. With an estimated 688 million people using the internet, China holds the distinction of having the world's largest number of internet users, outnumbering the entire US population two to one.[18]

All states, to varying degrees and for varying reasons, would like to exercise sovereign control to regulate what comes into their territory through the internet. The emergent virtual fences can be palpably felt in cyber space and a new "cybered Westphalian age" is emerging.[19] Every nation has a legitimate and compelling right to take measures to protect its national security, its economy and the lives of its people from the potentially coercive and corrosive effects of cyber space. This process is slow and is fraught with many complexities and ambiguities. However, in the near future, nations will be able to exercise sovereign control over internet content within their borders and will be able to regulate online activities in compliance with existing or future laws and legislations. Cyber space is inherently a man-made construct of systems of systems and has its genesis in the technology-enabled collaborative work of

17. Paul Mozur and Jane Perlez, "Gregarious and Direct: China's Web Doorkeeper," *New York Times*, December 2, 2014, http://www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper. html? _r=0. Accessed on January 20, 2017.
18. Euan McKirdy, "China's Online Users More Than Double Entire US Population," *CNN*, October 4, 2016, http://edition.cnn.com/2015/02/03/world/china-internet-growth-2014/. Accessed on January 20, 2017.
19. Maximilian Mayer, Mariana Carpes and Ruth Knoblich, *The Global Politics of Science and Technology - Vol. 1* (Berlin: Springer, 2014), p. 93.

A new generation cyber warriors, wielding cyber weapons, with specific military/intelligence objectives, will defend the national borders in cyber space. In so doing, they will deepen national borders.

academics, government sponsored research labs and some non-governmental organisations. The technological feasibility and political desirability of constructing virtual national borders is strong and is now manifesting in efforts to govern the cyber space within the respective physical borders.

Cyber Sovereignty and Cyber Forces Operating in the Cyber Domain

The basic role of the armed forces of any nation is to protect its sovereignty and territorial integrity. Historically, the military services tended to be divided by domain: the navy fights on the sea, the air force fights from the skies and the army fights on land. A nation's sovereignty extends to its land territory, internal water and territorial sea and air space over land territory and territorial sea. It also implies that in each domain, there is clear delineation of physical territory irrevocably associated with national sovereignty. Many nations now consider cyber space as a *mainstream domain* for military operations and have started developing capabilities and building capacities. For example, the establishment of the US Cyber Command in May 2010, is an overt assertion that the US directly exercises its sovereign rights over cyber space which it deems of utmost importance for its national security, economic vibrancy and democratic vitality. A new generation of cyber warriors, wielding cyber weapons, with specific military/intelligence objectives, will defend the national borders in cyber space. In so doing, they will deepen national borders. In effect, the notion of sovereignty in its Westphalian conception is being redefined in the context of cyber space and adopted with the specific purpose of protecting cyber space.

THE STUXNET EFFECT

The year 2009 was a defining year which marked the arrival of the first true cyber weapon, "Stuxnet'. A complex computer worm was developed

with the specific objective to penetrate and compromise a specific uranium enrichment facility in the Iranian city of Natanz. It was introduced into the facility's computer system with a USB drive. It went after the computers that controlled the centrifuges used to enrich the uranium and destroyed about 20 percent of them. It is believed that the perpetrators used four zero-day security vulnerabilities to spread around Microsoft's Windows operating system. The scope, scale and level of success of Stuxnet changed the whole notion of national security in cyber space. The transformation of a cyber weapon from an instrument of mass annoyance to an instrument of destruction, with the arrival of Stuxnet on the scene, forced the world to seek order in the disorderly world of cyber space. The success of Stuxnet changed the perception about cyber espionage, with realisation that serious strategic harm could be inflicted by a determined adversary leveraging cyber weapons. The acts of cyber spying or cyber espionage or even cyber theft suddenly started appearing as minor irritants in comparison to the possession of devastating and deadly power which could be wielded with unscrupulous skills remotely. Stuxnet also discredited the fallacy that being disconnected from the internet is a guarantee of security. Borders in cyber space are no longer an abstract construct and need to be clearly defined and delineated. The lack of sovereign control over cyber space remains a troublesome and worrisome concern to many. Many nations are still caught in the dichotomous debate between controlling the contents and supporting the notion of freedom over the internet.

The process of erecting virtual fences to regulate the flow of information and to prevent acts detrimental to national interests in cyber space has already begun. A 'Westphalian age' in cyber space is slowly but surely emerging, a direct ramification of a nation's resolve to exercise sovereign control over cyber space affecting its national interests. Some nations like Russia and China have already initiated the process to have precincts in cyber space. The delineation of sovereign rights and boundaries in cyber space has commenced, as evident from the efforts of many states to exercise the right of sovereignty over their part of cyber space. These efforts are crystallising into a new paradigm, supported by new technologies, modified institutional structures and

Initially, under the "Golden Shield" project, it was envisioned to build a comprehensive database-driven surveillance system capable of accessing every citizen's record as well as linking national, regional, and local security together.

manipulative psychological techniques. China is leading the way in its efforts to control the flow of information from outside as well as the information emanating and circulating within its borders. The internet made its appearance in China in the year 1994 primarily with an aim to bring in new technology to provide China with a competitive edge to bolster its economy. The event was analogous to the enactment of the 'open door policy' of 1979 to open the country to foreign trade and investment[20]. However, the open door policy also saw the influx of egalitarian ideas, and with the internet, came a multitude of diversified ideas including the concept of democracy. While the internet is indispensable in fuelling the Chinese economy, its reach and impact on the Chinese people is seen as a destabilising factor by the current political set-up. In order to balance between these two ends, the "Great Firewall of China" project, formally known as the "Golden Shield" project, was initiated, developed and operated. Initially, under the 'Golden Shield" project, it was envisioned to build a comprehensive database-driven surveillance system capable of accessing every citizen's record as well as linking national, regional, and local security together. The booming numbers of internet users necessitated various modifications and adjustments to its initial avataar. China has also been working on the "Next Generation Internet (CNGI)" project for developing an indigenous version of the internet.

The justifications and rationale for erecting fences in cyber space—as safeguards against social prejudice, against flow of false or fabricated information, against cyber espionage and for protection of the right to privacy, etc.—cannot be termed as controversial, regressive or authoritative. Several democratic nations have put in place regulating mechanisms to

20. "The Great Firewall of China", http://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/ Freedom OfInformationChina/category/great-firewall-of-china/index.html. Accessed on January 20, 2017.

prevent social disharmony, misuse or abuse of the personal information of their citizens and to protect their economic interests. States, as cybered entities with sovereign boundaries, will be able to defend themselves successfully against threats to their national interests.

In the realm of cyber warfare, the question of attributability and accountability is a piquant one. For one, in its present form, the internet does not offer a mechanism for verifiable identification of potential perpetrators.

India, as a tolerant, democratic and pluralistic society, has always stood for the right of freedom of expression. It has been reiterated at various forums that "India is committed to protecting, preserving and safeguarding freedom of expression and internet freedom and to strengthening them."[21] However, India has taken justifiable measures for removing content on the internet that endangers social harmony, public order or national interest. Section 69 A of "the Information Technology (IT) Act, 2008",[22] vests power with the government, if it feels necessary or expedient in the interest of the sovereignty and integrity of India, defence and security of the state or public order, to initiate actions to block access by the public to any information generated, transmitted, received, stored or hosted in any computer resource. Similarly, under many sections of the IT Act, various offences such as sending offensive messages through a communication service, generation of electronic mail for the purpose of causing annoyance or inconvenience, identity theft, cheating by impersonation by using the computer resource, violation of privacy, and cyber terrorism are punishable with imprisonment. In some cases, the act is punishable with imprisonment which may extend to imprisonment for life.

The dramatic success of Stuxnet in its ability to cause strategic harm has already firmed up the resolve, where there was already a loose consensus, to have borders in cyber space, with enforceable laws to protect the legitimate rights of countries and their citizens. The international efforts for the success

21. Sujay Mehdudia "Deputy NSA Questions US Control over Critical Net Resources", *The Hindu*, October 17, 2013.
22. The Information Technology Act, 2008.

of this, however, have to confront and overcome a myriad difficulties. In the realm of cyber warfare, the question of attributability and accountability is a piquant one. For one, in its present form, the internet does not offer a mechanism for verifiable identification of potential perpetrators. This has propelled individual states, wittingly or unwittingly, to adopt and use methods for controlling the web, without dwelling much on their authoritative, regressive and repressive nature. The clear delineation of cyber space under a formal agreement, with nation states exercising their right of sovereignty over part of the cyber sphere is not a distant possibility. The digital borders will provide security within their precincts against rogue intruders. The emergence of borders will also see the emergence of laws and rules applicable to cyber space which might bring order in the chaotic world of the internet.

Technological Pluralism and International Relations Narratives

Most of the developments in cyber space were conceived and executed outside the purview and supervision of government agencies and were not abided by any mandate of a government or constrained by a government decree. The collective development processes in cyber space were often fuelled by the technological breakthroughs or by the innovative adoption of spinoffs from earlier research and development efforts. Initially, these developments often had limited public acceptance and influence, and were deemed to be of minimal mass appeal, such that did not warrant regulatory oversight. As the new technology burgeoned and proliferated, the government agencies found themselves constrained in their capacity to put in place regulatory frameworks so as to prevent its abuse and misuse. Various companies and entrepreneurs became extremely wealthy and influential, dictating the terms on which their products could be used, with the commercial interests often trumping the national security concerns. The trans-global influence of such non-government companies in terms of information exchange, financial inter-connectedness and data sharing has facilitated the acquisition of power, the nature of which was once the sole purview of the state. It also signifies a shift in the approach towards

international politics, which is predominantly state-centric. The new technology and its ownership can expedite the shifting of the hierarchy of power in the international system, relegating the pre-existing actors to the margins.

When a private business entity, either as an individual or a corporation, becomes too powerful, it can influence the state to take a position to protect its commercial interest, instead of adhering to a position consistent with prevailing international norms. Some ICT companies, due to the power they wield, both within the country of their origin and outside, and the economic clout they have over financial markets, have the potential to impact the international order in a disruptive way. Some of the most powerful companies in the world today are ICT companies with market penetration across the globe. A large number of nations are peripherally or centrally dependent on the ICT infrastructure provided by these companies and their irrevocable dependence on these companies makes them vulnerable to these companies' malpractices and legitimate or illegitimate manipulations. The global commerce is witnessing a paradigm shift fuelled by "disruptive" technology that is radically changing the way organisations operate and the way business is conducted. On the superhighway of global information, the landscape of IR keeps changing which, in turn, impacts the states' policy formulation by focussing more on commercial factors, subordinating international commitments towards fostering harmonious and mutually beneficial relations.

A large number of nations are peripherally or centrally dependent on the ICT infrastructure provided by these companies and their irrevocable dependence on these companies makes them vulnerable to these companies' malpractices and legitimate or illegitimate manipulations.

In a multi-centric world of information networks, states are supported and supplemented by a consortium of ICT companies wielding enough influence and control to alter in varying degree, the states' obligations for international cooperation and assistance. The plurality of interests may prevent the development of effective state responses to the extent that the emergence of mutually collaborative strategies is stalled.

Alleged Russian Hacking During the US Presidential Election: A Case of Pervasive Entwinement of Cyber Space and International Relations

The 58th quadrennial US presidential election of 2016 was 'different' in more than one way than many previously held US presidential elections. In the past, much of the intense political drama—an intrinsic appendage of any democratic election—took place behind closed doors, but in 2016, every aspect of the presidential election was played out in the mainstream media or on the internet. The Republicans sprang a surprise by nominating as candidate Donald Trump, a shrewd and successful businessman who was politically naive and inexperienced. Pitted against a candidate far more experienced in politics, Donald Trump demonstrated an approach to campaigning for president that had no precedence in American political history. During the campaign, the stories of complex intrigues and political machinations featured incessantly on television, in the print media and on the internet.

The seismic political tremor caused by the surprise win of Donald Trump in the presidential election in November 2016 created ripples across the length and breadth of the US. When the Americans thought nothing could now surprise them, came the shocking revelation that the Russians, under direct orders from Russian President Vladimir Putin, had tried to influence the campaign. It was alleged that Russia tried to undermine public faith in the US democratic process, denigrate Democratic candidate Hillary Clinton and sabotage her prospects of electability and potential presidency. This speculative assertion gained traction as a possible Russian recourse to keep Donald Trump at the helm of the most powerful nation, owing to his stated policy to work with Russia and his pro-Kremlin rhetoric. Besides, it has been reported that Mr. Trump has business ties to Russia and Russian financial interests were closely linked with the successful presidential run of Mr. Trump

The whole Russian operation to influence the presidential campaign and to undercut Hillary Clinton's legitimacy was carefully orchestrated well in advance. On the eve of the Democratic National Convention on July 22, 2016, a collection of emails of the Democratic National Committee (DNC),

the governing body of the US Democratic Party, was published by WikiLeaks. The leaked collection included emails from key staff members of the DNC from January 2015 to May 2016, to chalk out a strategy to contain Bernie Sanders' popularity and to secure Hillary Clinton's candidacy as the Democratic presidential nominee.[23] WikiLeaks did not reveal the source of information; however, a hacker, using the moniker "Guccifer 2.0", claimed responsibility for the attack. According to leading US cyber security firms, the self-styled hacker Guccifer 2.0 is not a single operator but a loose group of Russian cyber criminals designated "Fancy Bear" and "Cozy Bear". The security firm ThreatConnect, after comprehensive investigation, reported that Guccifer 2.0 was using the Russia-based Elite VPN service to communicate with, and leak documents directly to, the media.[24] The rumour mills were abuzz with stories that the whole episode was orchestrated by the Kremlin, as part of its grand plan to facilitate Mr. Donald Trump's accession to the White House.[25] It has also been reported that "the Bill, Hillary and Chelsea Clinton Foundation" was breached by hackers suspected to have strong Russian connections.[26]

According to leading US cyber security firms, the self-styled hacker Guccifer 2.0 is not a single operator but a loose group of Russian cyber criminals designated "Fancy Bear" and "Cozy Bear". The security firm ThreatConnect, after comprehensive investigation, reported that Guccifer 2.0 was using the Russia-based Elite VPN service to communicate with, and leak documents directly to, the media.

Amid the growing clamour from Congressional Democrats for an investigation of possible Russian hacking in the US election, on December

23. US Office of Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, January 6, 2017, p. 2.
24. Threatconnect Research Team, Guccifer 2.0: "All Roads Lead to Russia," Threat Connect, July 26, 2016, https://www.threatconnect.com/blog/guccifer-2-all-roads-lead-russia/. Accessed on January 20, 2017.
25. Ellen Nakashima, "Is there a Russian Master Plan to Install Trump in the White House? Some Intelligence Officials are Skeptical," *The Washington Post*, July 27, 2016.
26. Michael Riley and Jordan Robertson, "Clinton Foundation Said to Be Breached by Russian Hackers," *Bloomberg*, June 23, 2016.

9, 2016, then President Obama ordered US intelligence to review evidence of Russian interference in the 2016 presidential election. It is ironical that the intelligence agencies that were entrusted with the responsibility of undertaking the investigation, now report to Donald Trump, considered to be the main beneficiary of the Russian meddling in the US election.[27] The outgoing president even warned that the US would retaliate for the Russian cyber attacks during the presidential election at a time and place of the US' choosing.[28] On December 29, 2016, the Obama Administration announced that as a retaliatory measure, there would be sweeping new sanctions against Russia that included the expulsion of 35 Russians.[29] In a statement, then President Obama said that he had issued an executive order that provides additional authority for responding to certain cyber activity that seeks to interfere with, or undermine, the US election processes and institutions, or those of US allies or partners.[30]

The Kremlin was quick to dismiss such allegations as baseless, unsubstantiated and amateurish and described them as part of a political witchhunt.[31] Speaking disparagingly of the US intelligence agencies, Russia termed these series of accusations as turning on a full-on witchhunt. Adding more twists and turns in the plot is the claim of the existence of a dossier which was compiled by former MI6 agent, Christopher Steele. It was alleged that Mr. Trump had potentially been compromised by the Russians during a 2013 trip to Moscow for the Miss Universe competition. Again, the Russian president dismissed the alleged links between Mr. Trump and Moscow

27. Spencer Ackerman and David Smith, "Barack Obama Orders 'Full Review' of Possible Russian Hacking in US Election," *The Guardian*, December 19, 2016, https://www.theguardian.com/us-news/2016/dec/09/us-election-hacking-russia-barack-obama-review. Accessed on January 20, 2017.
28. Julian Borger, "Barack Obama Promises Retaliation Against Russia over Hacking During US Election," *The Guardian*, December 16, 2016, https://www.theguardian.com/us-news/2016/dec/16/obama-retaliation-russia-hacking-us-election. Accessed on January 20, 2017.
29. Lauren Gambino, Sabrina Siddiqui and Shaun Walker, "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking," *The Guardian*, December 30, 2016, https://thevotingnews.com/obama-expels-35-russian-diplomats-as-part-of-sanctions-for-us-election-hacking-the-guardian/. Accessed on January 20, 2017.
30. Ibid.
31. Hyacinth Mascarenhas, "Russia 'Tired' of US Election Hacking Claims, Slams Intelligence Report as 'Baseless and Amateurish'," *International Business Times*, January 10, 2017.

and said that claims made in the dossier about salacious behaviour by Mr. Trump were obviously fake.

The alleged Russian intrusions into the American political system by leveraging cyber space and their malafide manipulations to influence the outcome of the presidential election strained the relationship between the two nations. It is an open secret that state supported, enabled, sponsored, and aided cyber operations are perpetuated across national borders and lack of consciously agreed-upon behavioural guidelines in cyber space could have unsettling consequences for the international order. Besides, the allegation about Russia meddling in American internal affairs and democracy is reminiscent of the Cold War rhetoric. The nostalgic sentiments that some Russian officials continue to hold for the Cold War saw the US discomfiture over these developments as assertion of Russia's resurgent political might.

Still, ICT is not considered a vital component of the global international order. It is time to focus on the efforts to embed ICT in the global socio-political-technical system for a truly trans-nationalised and globalised world of opportunity and equity.

CONCLUSION

The uneasy relationship between technology and power in IR appears more tumultuous when observed from the information age perspective. International relations, as a discipline, has theoretical explanations and practical suggestions on how to wield dominant political power, flaunt superior status and secure national interest. But, it lacks an expansive interpretation of the impact of technology. This is proving to be a limiting factor in understanding the impacts of technology on IR in more nuanced ways. Furthermore, in international relations, most of the theories are derived from empirical evidence from industrial technology and are woefully short in adequately factoring in the generative and causal effects of ICT. ICT expedites the flow of information and more shared information leads to more thrust and transparency, facilitating increased levels of interaction,

leading to outcomes that are mutually and synergistically beneficial. ICT also brings in an attitudinal change from adversarial to cooperative and collaborative among nations by debasing the reliance on 'hard power' and enhancing the role of 'soft power', and diffusing power to a larger number of actors in the international system. [32]

The modified norms of contemporary IR are more or less inconsistent with the traditional norms of states' behaviour due to the irrevocable diffusion of ICT into various IR processes, ranging from bilateral to global situations and transnational dimensions. The nature and degree of inter-dependence between countries witnessed a transformative shift in interest and expectations largely due to the information technological evolution.[33] Still, ICT is not considered a vital component of the global international order. It is time to focus on the efforts to embed ICT in the global socio-political-technical system for a truly trans-nationalised and globalised world of opportunity and equity.

32. Daniel R. McCarthy, *Power, Information Technology, and International Relations Theory* (Hampshire: Palgrave Macmillan, 2015), p. 23.
33. Mayer, n. 19, p. 116.